IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

CENTRIPETAL NETWORKS, INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	**Civil Action No. 2:18cv94**
	)	
CISCO SYSTEMS, INC.,	)	
	)	
Defendant.	)	

OPINION AND ORDER

Defendant, Cisco Systems, Inc. ("Cisco") filed a Rule 59(a)(2) motion for a new trial regarding the Court's rulings as to the '176 Patent and the '806 Patent as well as a new trial as to willfulness and damages. Cisco simultaneously filed a Rule 52(b) motion regarding direct infringement, damages, and an amended judgment as well as a Rule 54(b) request for partial judgment. There are overlapping findings of fact and conclusions of law applicable to Cisco's several motions and the Court will therefore rule upon all of Cisco's motions in this opinion and order.

For the reasons that follow, the Court **DENIES** each of Cisco's motions.

I. INTRODUCTION

As to infringement and validity, Centripetal and its experts relied on 1) Cisco's technical documents as interpreted by Centripetal's experts, 2) admissions in Cisco's pleadings, and 3) the testimony of Cisco's own engineers, principally Mr. Llewallyn and Mr. Jones, Cisco's

distinguished engineers. Cisco attempts to classify the Court's rulings as sua sponte, however, the most compelling evidence originated in Cisco's own technical documents introduced at trial by Centripetal and thus are anything but sua sponte. Cisco attempted to avoid the impact of its own technical publications by using animations prepared solely for trial as the basis for its expert testimony. The Court found that the animations misrepresented the functionality of the infringing products and found Cisco's retained experts' testimony unpersuasive as to infringement and validity as well as damages.

The four Centripetal patents which the Court found Cisco infringed, when combined, cover a broad spectrum of security software which promoted Cisco's security products from an also ran to a leader in the security marketplace. *See* PTX-1460. Cisco portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Cisco's Reply Brief in Support of 59(a)(2) at 17[1]. This was probably accurate as to hardware, but not as to the software required to operate it until Cisco began infringing the Centripetal patents on June 20, 2017.

The Centripetal '193 Patent, referred to at trial as the "FORWARD OR DROP EXFILTRATION PATENT," the technology from which is embedded in Cisco's switches and routers, enabled Cisco to proactively search for bad actors attempting to exfiltrate confidential data from the switches and routers which operate its networks. The '856 Patent, referred to at trial as the "ENCRYPTED TRAFFIC PATENT," the technology from which is also embedded in Cisco's switches and routers, enabled Cisco to proactively search for and find bad actors and malware in

[1] The Court is citing to the page numbers listed at the bottom of the briefs, not the page numbers assigned to the document by the Clerk's office.

the unencrypted portion of encrypted packets without decrypting them. Cisco repeatedly claimed that it was the first to possess this technology, but in fact it copied the technology from Centripetal. *See e.g.*, PTX-383; PTX-569; PTX-1009.

The '176 Patent, referred to at trial as the "CORRELATION PATENT," the technology from which is also embedded in its switches and routers, enabled Cisco to correlate its NetFlow intelligence with proxy data from multiple third party sources as well as to correlate intelligence from multiple sources within NetFlow. This enabled Cisco to proactively obtain up to date intelligence data for use in its infringing security software embedded in its switches and routers.

The '806 Patent, referred to at trial as the "RULE SWAP PATENT," the infringing technology from which is also embedded in its switches, routers and firewalls enabled Cisco to more efficiently and proactively transform up to date data and collate this intelligence into rules which are then used to detect and stop malware, bad actors (i.e. hackers) and exfiltration.

Accordingly, the patent claims within Centripetal's patented technology work in combination with one another on Cisco's hardware to transform the obsolete portions of Cisco's software from reactive to proactive. The four infringed patents then work together to furnish Cisco's customers with proactive security software throughout its network hardware, thereby contributing to Cisco's goal of transforming itself from a hardware supplier to a full-service network security supplier.

Although Cisco began infringing on June 20, 2017, it continued its copying of Centripetal's patents through 2019 and later, as is illustrated by its technical documents introduced at trial by Centripetal.

II. JUNE 20, 2017 AS THE DATE OF FIRST INFRINGEMENT AND A BASELINE TO COMPARE SALES

Cisco alleges that the Court ruled sua sponte in fixing the date of Cisco's first infringement. The evidence contradicts this claim. In determining the damages based on a reasonable royalty, the Court employed the hypothetical negotiation approach. Also known as the "willing licensor-willing licensee" approach, this calculation "attempts to ascertain the royalty upon which the parties would have agreed had they successfully negotiated an agreement just before infringement began." *Lucent Techs., Inc. v. Gateway, Inc.*, 580 F. 3d 1301, 1324 (Fed. Cir. 2009). "The date used for the occurrence of the hypothetical negotiation is the date that infringement began." *Centripetal Networks, Inc. v. Cisco Sys., Inc.*, 2:18-CV-94, 2020 WL 5887916, 56 (E.D. VA Oct. 5, 2020) (citing *Wang Labs., Inc. v. Toshiba Corp.*, 993 F. 2d 858, 870 (Fed. Cir. 1993)) [hereinafter October 5, 2020 Opinion]. Cisco stated in its opening statement that Encrypted Traffic Analytics, an infringing technology, came to the marketplace in June of 2017. *See* Trial Transcript [Docket Nos. 496-550] [hereinafter Tr.] at 221:19. As per PTX-1135, Cisco's own press release from June 20, 2017 marked the date of first infringement. Lance Gunderson, Centripetal's damages expert, explained why this date should apply to all four patents:

> "[T]hese patents really work in concert. They work together. They provide this operationalization of threat intelligence, this new concept that was a new and innovative concept brought about by Centripetal. So they really kind of worked together.
>
> . . . [T]hey have equal weight, each of them adds an important element to this operationalization.. . . [I]t seems like that they work in concert, and it's my opinion

> that any negotiation would have negotiated a license to all of the patents. Even some of the patents that actually issued afterwards. My understanding is the patents were actually filed for prior to this hypothetical negotiation, they would have been known, and these reasonable actors would have licensed everything." Tr. 1445:14-1446:2.

Cisco's damages expert, Dr. Stephen Becker, agreed that June 20, 2017 would be about the date of the hypothetical negotiation. *See* Tr. at 2993. Further, Becker agreed that the date of first infringement for at least some of the patents at issue would be June 20, 2017:

> Q: And you agree that the start date of damages for purposes of this case, as it relates to the various [four] patents, begins starting June 20 of 2017; is that right?
> A: Yes. It's not every single patent and every single product, but generally that's when it starts. Tr. 2964:4-8 (cross-examination by Ms. Kobialka).

The Court found the date of first infringement to be June 20, 2017. *See* Tr. 725:3-8 (Dr. Michael Mitzenmacher stating this as the date of first infringement); *see also*, Tr. 1534:17 (Cisco cross-examining Mr. Gunderson and confirming his stated date of first infringement was June 20, 2017). The damages are calculated by positing what would be agreed upon at a hypothetical negotiation. *See Lucent* at 1324. Because all the infringing patents work in concert—and because three of the four infringed patents had been granted and the fourth filed for prior to June 20, 2017 and would have been known—it is reasonable to determine that all four patents would be negotiated for licensing at the same time. *See* Tr. at 1445:14-1446:2. As Mr. Gunderson stated in his testimony:

> You look for the date of first infringement. You have a variety of patents, it's the same month that the '193 Patent was issued. There were also some accused products that were sold that month. So there's not a lot of dispute about this date that I'm aware of. They would negotiate a reasonable royalty for all [four] patents, in my opinion, at this time. Tr. 1444:24-1445:5. (direct examination by Ms. Kobialka).

This date was put forth by Centripetal, based upon a Cisco Publication PTX-1135, acknowledged by Cisco's own damages expert during his trial testimony, and certainly was not a *sua sponte* ruling of the Court as claimed by Cisco.

III. DAMAGES - GENERALLY

In its damages case Centripetal relied upon 1) an apportionment formula approved by the Federal Circuit, 2) the only royalty rate cited by either party previously utilized in an infringement claim relating to the same family of patents, and 3) sales data obtained from Cisco which corroborated the damages claimed by Centripetal and accorded with economic reality.

Cisco presented a damages expert whose theory lacked any precedential or evidentiary support in patent law, and was completely devoid of economic reality.

The Court found Centripetal's evidence on infringement, validity, and damages credible and persuasive. The Court found Cisco's defenses objectively unreasonable and in many areas not credible, as well as finding its conduct willful and egregious in infringing the four patents. The Court found that Centripetal did not prove by a preponderance of the evidence that the '205 Patent was infringed by Cisco. The '205 Patent dealt primarily with a method of 'tapping' telephones and was used mostly by law enforcement to record such calls. This is the opposite of the functionality of the infringing products, Cisco never claimed the ability to make, use or sell products based upon the '205 Patent technology. The '205 Patent had no impact upon the Cisco sales data analyzed by the Court or the Court's computation of any form of damages.

IV. MAKING, SELLING AND USING THE INFRINGING PRODUCTS IN COMBINATION IN THE UNITED STATES AND ELSEWHERE AND DAMAGES

Cisco challenged the Court's calculation of damages in both its Rule 52(b) and 59(a)(2) motions. In the introduction to its brief in support of its Rule 52(b)/54(b) motion, Cisco argued the following: "It is undisputed that the accused products are sold separately and that (for instance) Cisco switches, routers or firewalls may be bought and used without buying the other products in the combined systems found to infringe." Cisco's Brief in Support of its Rule 52(b) Motion [Docket No. 628] at 2. "Centripetal did not show, and the Court did not find, that every one of the accused products would meet claims' limitations when sold or used by themselves." Doc. 628 at 11. The evidence demonstrates that the accused products were made and sold to be used in the United States embedded with and in combination with the infringing technology.

Cisco's hardware - i.e., switches, routers, and firewalls - cannot operate without software, and the software that constituted Cisco's operating systems contained Centripetal's patented technology, which Cisco thereby infringed. Further, Centripetal's experts testified that it was Cisco's post June 20, 2017 infringing software that was embedded in Cisco's switches, routers, and firewalls. Multiple technical documents introduced in evidence by Centripetal, but published and circulated by Cisco itself, illustrated in diagrams and explained in text precisely how the infringing software functioned in the Cisco networks, which operated through its switches, routers, and firewalls. Thus, Centripetal presented credible and persuasive evidence of infringement corroborated by Cisco's own technical publications and the testimony of its own employees; including Mr. Llewallyn and Mr. Jones who were designated "distinguished engineers," as well as by Dr. Schmidt, a retained Cisco expert. Cisco for its noninfringement evidence relied upon

animations created for trial, upon which their independent experts in turn relied in forming their opinions. The Court found the animations misrepresented the functionality of the infringing technology and found the testimony of Cisco's independent experts unpersuasive and in many instances not credible, resulting in a finding that Cisco's defenses were objectively unreasonable.

Cisco did not present any evidence that contradicted its own documents, employees, and Centripetal's experts. In fact, none of the authors or presenters of its technical documents were called as witnesses. Instead, Cisco tried to avoid responding to its own publications by creating misleading animations for use at trial. Cisco presented the testimony of Dr. Becker on its "lack of product combination" defense. Dr. Becker, its damages expert, testified as follows:

> Q. And just to be clear for the record, does that $13.4 billion represent the revenue from Cisco customers who purchased the required combination of products for the '856?
> A. No. No. In fact it's, it is all of the revenue from all 98,800 customers, which we could see from looking at the StealthWatch data we know that the vast, vast majority of those customers just have the switch. They're just using the switches and routers, they're not also using this Cisco security product in the form of this, of StealthWatch.
> Q. Did Mr. Gunderson account for the fact that the accused switches and routers "can" be sold separately from the other products required for these accused combinations?
> A. No.
> Q. Do you know whether Mr. Gunderson had access to the same data that you had with respect to these revenue figures?
> A. He did. He has all the same data that I have and he could have looked at these combinations and didn't.
> Q. If Mr. Gunderson had considered the required combination of products, what would that have done to his royalty base in your view?
> A. Well, I think we know that mathematically his base would have been a very, very small fraction of what it was since well-less than five percent of the customers, the data would indicate, have the combination that's required. Trial Tr. 2879:5-2880:3 (Dr. Stephen Becker's testimony) (emphasis added).

However, testimony from Cisco's first independent expert to testify, Dr. Doug Schmidt, contradicts Dr. Becker's damages theory. Dr. Schmidt's factual testimony confirmed explicitly that ETA was embedded in Cisco's Accused Switches:

> THE COURT: Well, I read something that said ETA was embedded in the switch. What does that mean?
> THE WITNESS: That's correct. That's what it just said here at the bottom. The last sentence that's on the screen right now says that.
> BY MR. GAUDET (Cisco counsel):
> Q. What part of ETA is embedded in the switch?
> A. The part that collects the Initial Data Packet and the Sequence of Packet Length and Times.
> Q. Is that what it says in this document?
> A. That's exactly what it says in this document, yes. Trial Tr. 2131:12-22. See also PTX-963 illustrated.

Executive Platform

Cisco Extends Encrypted Traffic Analytics to Nearly 50,000 Customers

Scott Harrell
January 10, 2018 - 2 Comments

Here. Cisco has solved one of the biggest challenges facing the security industry – and now thousands of Cisco customers can start using this breakthrough new network security technology.

Back in June, Cisco announced Encrypted Traffic Analytics – a breakthrough technology that identifies malware in encrypted traffic, without having to break apart the packets and inspect the contents. This unique solution allows security teams to balance security and privacy – and significantly reduce costs along the way.

Since then, Encrypted Traffic Analytics – or ETA – has been in early field trials with customers around the world. The feedback has been incredibly positive, and we're now moving into general availability. But, as a great man once said, there's one more thing … and we think it's a big deal.

Today, we're also expanding support for ETA beyond campus switching to the majority of our enterprise routing platforms, including our branch office router (the ISR and ASR) and our virtual cloud services routers (CSR).

Plaintiff's Trial Exhibit
PTX-963
Case No. 18-cv-00094-HCM

Dr. Schmidt additionally confirmed in his factual testimony that Cisco's infringing products were sold in combination:

> BY MR. GAUDET (Cisco counsel):
> Q. Let's be clear: Does Cisco have any customers who would only buy this product and not have the other products that are actually designed to prevent malicious packets from coming in?
> MR. ANDRE: Objection. Lacks foundation. He doesn't know.
> THE WITNESS: I do know.
> BY MR. GAUDET:
> Q. Do you know that, Dr. Schmidt?
> A. Yes, of course. Only if those customers are extremely looking forward to having their networks hacked. Good network administration, Your Honor, relies on what's called layered defense, where you have firewalls, you have tools like StealthWatch. This is a comprehensive technique. Comprehensive set of products.
> Trial Tr. 2130:7-20.

While the Court rejected Dr. Schmidt's expert opinion on infringement and invalidity, when reckoning with competing testimony it is within the purview of the Court as the trier of fact to determine which witnesses and what testimony or portions thereof are to be accepted as credible. *See Sartor v. Arkansas Natural Gas Corp.*, 321 U.S. 620, 627 (1944) ("The rule has been stated that if the Court admits the testimony, then it is for the [trier of fact] to decide whether any, and if any what, weight is to be given to the testimony.") (internal quotations removed); *see also, In re Methyl Tertiary Butyl Ether (MTBE) Prod. Liab. Litig.*, 739 F. Supp. 2d 576, 604 (S.D.N.Y. 2010) ("In general, a [factfinder] is not required to choose between adopting or rejecting an expert's testimony wholesale; it is free to accept or reject expert's opinions in whole or in part and to draw its own conclusions from it.")

Of course the software programs, such as StealthWatch, "can" be sold separately, as the sales data twice supplied by Cisco illustrates clearly. Customers who already owned Cisco hardware, as well as the outdated Cisco software such as the older versions of StealthWatch, would

only need to purchase the newer infringing software so long as the customer's existing hardware was compatible. The Court found that the preponderance of the evidence established that the sales data for the switches, routers, and firewalls, produced during pretrial discovery and again in more detail at the damages hearing, listed by Cisco were embedded with software which infringed the four Centripetal patents. Cisco was asked to produce sales data on its "accused products," which Centripetal proved were "embedded with its patented software." Dr. Becker's testimony did not refer to the sales data produced in response to the Plaintiffs and the Court's requests for sales data of the "accused products." Cisco never produced any other evidence that its "accused products," as identified in its pretrial sales data production or its second production at the Court's damages hearing, did not contain the infringing software, while Centripetal presented a preponderance of evidence that it did. The Court inferred that Cisco's failure to produce such evidence, even when Dr. Becker was invited to do so by the Court, is proof that the sales data twice presented by Cisco did contain the infringing software. At no time did the Court request that Cisco produce the sales data for all Cisco's hardware and software, as Dr. Becker's testimony might suggest, but rather sales data relating to the "accused products."

Not only is Dr. Becker's testimony contrary to the preponderance of the evidence in the case, but he also misrepresents the testimony of Centripetal's expert, Mr. Gunderson who stated as follows:

> BY MS. KOBIALKA (Centripetal's counsel):
> Q. And can we go to Slide 45? And can you just provide your key takeaways in terms of your opinion for the hypothetical negotiation?
> A. It's my belief that the Centripetal/Keysight patent license is the best available information we have and it's something that I did use. The asserted functionalities are contained within the switches, the routers, firewalls and the other accused products and they work in concert. And apportionment method needs to measure

value provided to Cisco, and so that's what I believe happened with Dr. Striegel's analysis. The asserted functionalities are of critical importance to Cisco and end-users, and I think we went through a series of schedules that showed that importance. And finally, I believe that Georgia-Pacific factors support the royalty and are consistent with the Keysight license agreed rate.[2] Trial Tr. 1525:10-25 (Lance Gunderson's testimony).

Q. "ETA Impact on Security Bookings." And if you can explain here how this informed your opinion?
A. So it says "We're also embedding it in our products right and you can look at like when we acquire StealthWatch. It's now part of what we're doing at Cat 9000." So this is really talking about the importance of ETA and the fact that it impacts their bookings. And bookings, I think, means their sales, essentially. And it's really a revenue impactor, is what they're saying. Trial Tr. 1472:17-25 (Lance Gunderson's testimony); *see* PTX-31 at Bates No. 006.

Q. Okay. I'd like to turn to the royalty base, and we can go to Slide 36. What did you use for coming up with your royalty base?
A. Well, again, in terms of the royalty base we need to look at what is infringing, and we have to start out with what constitutes infringing. And my understanding of the statute is, making it, using it, importing it, offering it for sell, and selling. Those are the -- that's the way the statute reads. And so I always keep that in the back of our mind as we're looking at what the royalty base is. No. 2, the asserted patents are system claims, and so they're for a system comprising a variety of different things. And they're computer-readable medium claims which, in my mind, is software. It's really software that's on the system that makes the patents go, essentially. And then thirdly, the asserted functionalities are embedded in the switches, routers, and firewalls through this source code. This infringing code that is throughout the system. Trial Tr. 1499:18-1500:10 (Lance Gunderson's testimony).

Q. And the 9300 Series the first -- it looks like it's always included Encrypted Traffic Analytics, and that's the first model to do so?
A. Yep. The way it's sold here is that it's always included, yep.
Q. And in addition there was other evidence at trial, you also saw that ETA was also part of the Catalyst 9000 switches?
A. Yes. Trial Tr. 1461:20-1462:2 (Lance Gunderson's testimony).

---

[2] Centripetal analyzed its damages using the *Georgia-Pacific* factors, and, under those parameters, Keystone was the only license transaction in which Centripetal had been involved. It sought additional licensing information from Cisco, but none was forthcoming. In answering Centripetal's interrogatory, Cisco stated that it was "not presently aware of any patent license agreements that relate to the functionality of accused instrumentalities, nor is Cisco aware of any other license relevant to the evaluation of a reasonable royalty of damages in this case." Trial Tr. 1478:23-1479:2 (Mr. Gunderson quoting Cisco's interrogatory response). However, Cisco's exhibit, DTX-729 at page 5, shows that Cisco had licensed StealthWatch from Lancope for approximately two years before Cisco purchased Lancope in 2015. It is not clear if Cisco was contending that the Old StealthWatch was not comparable to the post-2017 7.0 version of StealthWatch or what the reason was for omitting the StealthWatch license.

MS. KOBIALKA: If we could look at PTX-1507?
BY MS. KOBIALKA:
Q. Mr. Gunderson, can you describe what that document is?
A. It's a very simple -- excuse me --
THE COURT: Let me get to that.
MS. KOBIALKA: Sorry. Maybe we can highlight the date at the bottom.
THE COURT: This is 2017?
MS. KOBIALKA: That's correct.
THE COURT: All right. You may proceed.
BY MS. KOBIALKA:
Q. Mr. Gunderson, could you tell us what this document is?
A. It's very similar to the last document that we had. Last document was talking about switches, this is talking about routers. Integrated Services Router. And it has a couple of different generations of routers, and then it's comparing it to the Cisco 4000 Series of routers. And it's an attempt to upsell, to get the current clients of Cisco to buy this new and innovative router that has this great technology on it.
Q. Okay. And I see a blue button up on top, says "How To Buy". Do you see that as well?
A. Yes.
Q. Okay. So this is evidence of how Cisco offers to sell and sells its routers, right?
A. Yes. They point out the benefits, and they're trying to get their existing customers to upgrade and put in a Cisco 4000 Series router.
MS. KOBIALKA: Okay. Now if we could highlight the second row, which is Cisco IOS XE Open operating system all the way across. Then if we could go down to couple it says Cisco DNA Center[3], Centralized Management.
BY MS. KOBIALKA:
Q. And could you just explain what we're seeing here with the check box under the 4000 Series for these?
A. So it shows no checks on the first two generations and then it had a check box that says that's included. So it's got the new IOS that's being accused here as the DNA Center, Centralized Management System. So there's a check box there. It has – you know, you look further down it says Cisco DNA Assurance Network Monitoring. It has a variety of the accused functionality that is included in the Cisco 4000 Series.
Q. If we could turn to the next page of this document? I'd like to just point out the two rows at the bottom. Says "Cisco StealthWatch Enterprise and Encrypted Traffic Analytics." Does this show that also those things come with the Cisco 4000 Series Integrated Services Router?
A. Yes. You can see that those check boxes are there and they come with it, it appears, automatically.
Q. Is this just one example like the other one with the switches of what you have seen in terms of how Cisco sells and offers to sell these products?

[3] There is a glossary of abbreviations attached as Appendix A of the Court's Opinion and Order dated October 5, 2020.

> A. Yeah. So even though they might have a separate charge, sometimes for StealthWatch, for example, they're selling it as one product. These all work together. And that goes to my point: This is, they're really -- they're really trying to sell everything together and to sell a solution rather than just sell individual products. Even though they might charge differently for them, they're selling them together. Trial Tr. 1462:5-1464:13.

The Court found this testimony presented by Centripetal credible, persuasive, and in accord with the preponderance of the evidence. Mr. Gunderson relied to a great extent upon Cisco's own publications, which corroborated his opinions. There is no equivalent corroboration from any source for Dr. Becker's opinions, which the Court rejected. In addition to the evidence Centripetal presented relative to the accused technology being embedded in Cisco's switches, routers and firewalls, Cisco effectively admitted as much in its discovery responses. When asked to produce data regarding its sales of accused products it included specific amounts for its switches, routers, and firewalls through December 31, 2019 in response to Centripetal's pretrial discovery. In its attempt to tailor its damage awards to the evidence, the Court requested that Cisco refine its sales data to a month to month outline and update it to begin in July of 2016 and extend it through the trial which began on May 8, 2020. The Court also invited Cisco's damage witness, Dr. Becker, to furnish any data supporting his damage theory, where at one point he stated that less than five percent of all sales involved sales in infringing combinations. The Court rejected his five percent figure since Cisco offered no sales data to support it, and it conflicted with Centripetal's evidence to the contrary that the Court found reliable. Cisco's sales data produced for pretrial discovery was the same data produced when the Court requested updated sales records. Cisco merely updated the sales records. At no point did Cisco dispute which accused products should have been included or excluded, nor did they at trial contradict with evidence to Centripetal's characterizations that the accused products contained in the sales data infringed.

With regard to damages, the Court accepted Centripetal's theory of damage calculations which was based upon Dr. Striegel's apportionment and Mr. Gunderson's and Mr. Malackowski's application of the financial data. The Court did not base its damages calculations upon the comparative sales data before and after June 20, 2017 produced at the June 25, 2020 Court hearing on damages, but upon the *Finjan* and *Ericsson* cases in which the Federal Circuit expressly approved the damages theory employed by Centripetal. *See Finjan, Inc. v. Blue Coat Sys., Inc.*, 879 F. 3d 1299, 1310 (Fed. Cir. 2018); *Ericsson, Inc. v. D-Link Sys., Inc.*, 773 F. 3d 1291, 1266 (Fed. Cir. 2014). The Court also analyzed the *Georgia-Pacific* factors in its opinion. *See* October 5, 2020 Opinion at 126-49; 164-65.

The Court did seek further evidence supporting damages from both parties in an attempt to resolve the vast difference in the approaches and results presented by the opposing parties. The request by the Court to Dr. Becker began on Trial Tr. 2968:1 and continued through Trial Tr. 2979:5. The Court only had six (6) months of sales data, beginning January 1, 2017, preceding the June 20, 2017 date of first infringement. The Court found that an additional six (6) months of sales data would assist it in determining whether the data would support Centripetal's theory of damages or that of Cisco. The key portions of the Court's request for additional data is set forth as follows:

> THE COURT: All right, Dr. Becker. With respect to that data, what the Court needs, to try to figure out what's going on between these various opinions, is the sales of the products in the '176, the '193, the '205, and the '806. I need the monthly sales of those products beginning in 2016, June of 2016. You can't begin them in the middle of a month, so let's say you'll begin them July '16, July of 2016, with those four patents. I want the monthly sales of the predecessor products for the period of one year prior to June 20, 2017, so that would include the entire month of June, for the predecessors of the accused products because the products are accused beginning June 20th. And when I say, "the accused products," I want to include the sales of all products after that date, on a month-to-month basis, which included the products – all the features accused by the plaintiff. Trial Tr. 2968:17-2969:7.

The Court then asked Dr. Becker to furnish the sales figures based upon his damages theory:

> THE COURT: ...Then I'd like for you to do the same thing with what you considered to be the relevant products, which -- and you didn't consider, for example, in some cases, the routers and switches to be relevant products, so I just want the sales of what you considered to be the relevant products, which included, for example, StealthWatch in some instances, but it didn't include the routers and switches. Trial Tr. 2970:23-2971:4.

Cisco only produced one set of documents in response to the Court's request. It did not produce any compilation of sales figures to support Dr. Becker's theory of damages.

The Court dealt specifically with the '856 Patent because it was granted after June 20, 2017.

> THE COURT: All right. And for the '856 Patent, that patent -- well, I would really just ask for the same data on the '856 Patent, but the patent wasn't granted until after the relevant date. It was granted in '18, and the relevant date is June 20 of '17, so just get me the same figures for that patent on a monthly basis.
> THE WITNESS: Right. I think, to the extent that -- the data that's collected for these other four patents will -- just glancing at the list, I think it will overlap with the '856, and I think, to the extent that we are able to collect the data and get it to you related to the other four, it will cover everything you're asking for on the '856. Trial Tr. 2973:5-16 (Dr. Stephen Becker's testimony).

In its Reply (Rebuttal) brief in support of its Rule 59(a)(2) motion on Doc. 635 p. 15, Cisco stated:

> Likewise, the Court put strict limits on this follow-up testimony from Dr. Becker, instructing Dr. Becker that he was "not to discuss your testimony with anyone between now and the time that you're prepared to deliver the data to the Court," and cautioning Cisco's counsel that it was "to use good faith in limiting themselves to just furnishing the source of the data." Trial Tr. 2978:4-25.

What Cisco describes as "strict limits" applied to barring new damages theories (models). There were no limits on the data to be supplied.

> THE WITNESS: Yes. There's a particular model, for example, that I think the record would show doesn't actually -- won't work with any of the security products, but I think I have an understanding of what you want, and we will work to get that done.
> THE COURT: Well, and you're not limited by what I ask for.
> THE WITNESS: I understand.
> THE COURT: If there's something else along these lines -- you know what I'm thinking about -- that you think would be helpful, go ahead and include it. But I've got to resolve this tremendous difference in --
> THE WITNESS: I understand.
> THE COURT: -- what each side is coming up with, and I'm trying to think how I can best do that. Trial Tr. 2977:2-17 (Dr. Stephen Becker's testimony).

What the Court requested and received was updated sales data through June 2020 plus comparative data for the year preceding the date of the alleged first infringement on June 20, 2017. The sales data, if any, which Dr. Becker used in his damages calculations was not furnished. The Court already had the total sales of the accused products from January 1, 2017 to December 31, 2019.

On page 9 of Doc. 626, its initial memorandum in support of its Rule 59(a)(2) motion, Cisco states:

> In its Opinion and Order, the Court used the sales data from June 2016-June 2017 in a way that Centripetal never had. The Court set forth a table summarizing "Centripetal's estimates regarding Cisco's revenue increase for the infringing products, after the date of first infringement, as compared to the predecessor products sales for the fiscal year before June 20, 2017." Order at 139-140.
>
> And further stated on page 10 of Doc. 626:
>
> Comparing product sales from June 2016 – June 2017 to product sales over the subsequent three-year period was not a damages model that Centripetal presented to the Court. Nor was it a model that Centripetal (via its damages experts Mr. Gunderson or Mr. Malackowski) had ever suggested would be appropriate.
>
> These allegations are not supported by the evidence.

As previously noted, comparative sales before and after June 20, 2017 was not the damages model the Court utilized. It was evidence, which along with Cisco's marketing documents, corroborated the enormous increase in sales resulting from Cisco embedding Centripetal's software in its switches, routers, and firewalls. The Court also considered sales data as corroborating evidence in accord with *Georgia-Pacific* factor number 11, the comparison which originated with Centripetal's damages expert, James Malackowski, who stated:

> I calculated the averages sales for the predecessor products; I set that as the baseline; and then I calculated everything that was above the baseline for the accused sales to show you the rate of growth. Trial Tr. 3437:16-19

Centripetal electronically filed a group of seven (7) exhibits outlining the data which was the basis for his above quoted testimony at the damages hearing. Mr. Malackowski received the underlying data from Cisco on June 18th and 19th, 2020. Cisco never objected to the Court's request for this data at trial, nor did it object to the manner in which the data was utilized during the damages hearing at which Centripetal compared the dollar amounts of sales of the predecessor products with the dollar amounts of the alleged sales of infringing products. Cisco's only objection to the data was the manner in which the sales of the predecessor switch products were computed.

> BY MR. JAMESON (Cisco counsel):
> Q. And, Dr. Becker, was there daylight between you and Mr. Malackowski with respect to what constituted the predecessor products to the 9000 series one?
> A. Yes. There's substantial -- there's a substantial difference. Set aside this question of the update between June 18th and June 19th, the slides that Mr. Malackowski just presented, which have the updated data in them, are comparisons that only treat the Cisco 3000 series switches as predecessors to the Catalyst accused 9000 series switches, and that is just -- frankly, it's inconsistent with the facts and, I think, creates a very significant difference in the picture that is painted with respect to the sales of the predecessor switches versus the accused switches. Trial Tr. 3441:14-3442:1.

As the Court noted in its opinion, the technical predecessor issue may have been caused by Cisco arguing at trial that the 3000 series of switches, not the 6000 series, was the "design"

predecessor to the 9000 series. However, as to damages, the 6000 series should be treated as a predecessor product. The Court reduced the differential by approximately $200,000, but the differential in sales of the infringing Cisco products was nonetheless $5,575.4 billion, which corroborates Centripetal's apportionment theory and royalty rate for damages. The $5,575.4 billion is not an exact figure, but it was only used to corroborate the multi-billion dollar damages figure claimed by Centripetal, not to actually compute damages.

Dr. Becker's bottom line was to value all five (5) patents then in issue at $3,014,561.00. It is instructive to compare this number with PTX-584, a Cisco technical document from 2018 that states the average cost of a single data breach is $3.86 million, which is more than Dr. Becker's value for all of the patents combined. However, the cost of a data breach helps to explain why Cisco's customers paid it over twenty (20) billion dollars for its infringing security products for the period from June of 2017 to June of 2020.

Very shortly before the Court's damages hearing on June 25, 2020, Cisco filed sales data separating sales in the United States from overseas sales in an effort to reduce the royalty base. This deepens the enigma Cisco created by its tactics in producing sales data in the United States and overseas while denying that any sales of accused products have been proven by Centripetal.

Cisco took similarly inconsistent positions during the trial regarding infringement and validity attempting to use the case of *01 Communique Lab., Inc. v. Citrix Sys., Inc.*, 889 F. 3d 735, 742-43 (Fed. Cir. 2018) to support its arguments. The *01 Communique* case did not support Cisco's inconsistent positions on infringement and invalidity then or on damages now. Cisco has cited no

other authority that supports the inconsistent positions regarding its sales data and making, using, and selling the accused products which it attempts to argue.

The authority cited by Cisco in support of its defense to damages based upon the worldwide sales of the accused products is inapposite. In fact, the case relied upon by Cisco (*Power Integrations, Inc. v. Fairchild Semiconductor Int'l., Inc.*, 711 F. 3d 1348, 1371 (Fed. Cir. 2013)) makes clear that where products are made in the United States, the patent owner is entitled to damages for direct infringement based on overseas sales. *Power Integrations* discusses whether a party is entitled to damages for infringement that occurs outside of the United States. *See* 711 F. 3d at 1371 ("[T]he underlying question here remains whether Power Integrations is entitled to compensatory damages for injury caused by infringing activity that occurred outside the territory of the United States."). As the court in *Power Integrations* notes, infringement cannot happen entirely outside of the United States: "[T]he entirely extraterritorial *production*, use, or sale of an invention patented in the United States is an independent, intervening act that, under almost all circumstances, cuts off the chain of causation initiated by an act of domestic infringement." *Id.* (emphasis added). Centripetal, however, did not seek damages for extraterritorial products. Thus, *Power Integrations*' only value in this instance would be to show that the sales for infringing products *produced* in the United States but used or sold extraterritorially do indeed infringe.

There is support for the Centripetal's damages award for worldwide sales due to direct infringement under § 271(a). The Supreme Court's decision in *WesternGeco LLC v. ION Geophysical Corp* allowed damages for foreign sales when there is infringement under subsection § 271(f)(2). 138 S.Ct. 2129, 2139 (2018). As the Supreme Court states, "Taken together, §

271(f)(2) and § 284 allow the patent owner to recover for lost foreign profits . . . when the patent owner proves infringement under § 271(f)(2)." *Id. WesternGeco* suggests that a similar act of infringement under § 271(a), where an infringing product was made in the United States but sold internationally, would qualify a plaintiff to the same damages for foreign sales set forth under § 271(f)(2). *See, e.g., Plastronics Socket Partners, Ltd. v. Dong Weon Hwang*, No. 218CV00014JRGRSP, 2019 WL 4392525, at *5 (E.D. Tex. June 11, 2019) ("[T]hese instances would constitute infringement under § 271(a), and thus, under the reasoning of *WesternGeco*, would be compensable even if the sale causing damage ultimately occurred abroad.").

Cisco never offered any persuasive evidence to counter Centripetal's proffered testimony and its own response to requests for admissions evidencing that the accused products were made, used, and sold in the United States and the Court found for Centripetal on this issue. *See* Opinion at 32, 86, and 100; *see also*, PTX-1409 at 5-6; PTX-1932. Further Cisco never offered evidence to rebut Centripetal's preponderance of the evidence that its infringing software was not embedded in its traditional hardware and sold in combination with it and when it was asked in pre-trial discovery and later by the Court to produce the data explaining the sales of its "accused products" it produced sales data which included "accused products" containing the infringing technology. Cisco's only response to Centripetal's evidence was to say it's hardware "can" be sold separately, which is insufficient to challenge Centripetal's comprehensive presentation.

Accordingly, the Court **FINDS** that Centripetal has proven that the sales data of the "accused products" which it produced was embedded with and sold in combination with the infringing technology continued Centripetal's Patents '806, '856, '176 and '193. The Court further

FINDS that Centripetal accurately computed its damages based upon the correct data supplied by Cisco using a proper model including apportionment and the *Georgia-Pacific* factors approved by the Federal Circuit, and that Centripetal is entitled to damages based upon worldwide sales as Centripetal proved direct infringement of the four patents remaining in issue. Insofar as Cisco's Rule 59(a) and 52(b) and 54(b) motions relied upon arguments to the contrary they are denied.

V. MR. LLEWALLYN'S AFFIDAVIT AND PATENT '856

Cisco's motion pursuant to Rules 52(b) and 54(b) challenged the Court's finding that the '856 Patent was directly infringed. Cisco attached affidavits from Mr. Daniel Llewallyn and Mr. Peter Jones, its distinguished engineers, to its initial Rule 59(a)(2) motion for a new trial. Llewallyn's affidavit and its attachments were marked as Exhibit A to Doc. 625. Cisco presented Mr. Llewallyn at trial in its defense of the claimed infringement of the '856 Patent. Centripetal relied on Llewallyn's trial testimony in its infringement case particularly regarding Patent '856 referred to at trial as the Encrypted Traffic Patent. In its post-trial Rule 59(a)(2) motion Cisco seeks to use Llewallyn's affidavit to support its noninfringement argument with regard to the '176 Patent which was referred to at trial as the Correlation Patent. Trial Tr.884:25.

However, Llewallyn's expertise was related primarily to the old StealthWatch which he helped develop while employed by Lancope, which was purchased by Cisco. Cognitive Threat Analysis (CTA) was later integrated with an updated version of StealthWatch in 2017, and Mr. Llewallyn had only a basic familiarity with Encrypted Traffic Analysis (ETA) or CTA at the time of his trial testimony.

BY MR. BAIRD (Cisco counsel):

Q. Okay. Now we're showing this with Cognitive Threat Analytics integrated with StealthWatch. When did that happen?
A. The Cognitive Threat Analytics integration was in 2017. It was in version 6.10.3.
THE COURT: This represents Version 10.3 of StealthWatch?
THE WITNESS: 6.10.3, I'm sorry.
THE COURT: 6.10.3?
THE WITNESS: That's correct.
BY MR. BAIRD:
Q. So this is --
THE COURT: What do all those numbers stand for?
THE WITNESS: Oh, that's just our numbering system.
We have like our release levels. We'll call it 6.10, 6.11 as we move on. But if you have a minor release in between the bigger releases, that's where the third number comes in. So we had a 6.10.1, a 6.10.2. That's just our numbering system for our releases.
THE COURT: And each of those, the last number would be a minor release; the one before that would be a major release, is that it?
THE WITNESS: Exactly. Exactly. And if it's a really, really big change we would change this to 7.0.
THE COURT: Okay. When did you get to level 6?
THE WITNESS: That was in around 2012 I think it is when we started shipping 6.0.
THE COURT: And when did you get to 6.10?
THE WITNESS: That was in the 2017 time frame.
THE COURT: Okay. You may proceed. Trial Tr. 2148:8–2149:11.

Mr. Llewallyn testified that he had never heard of Centripetal:

BY MR. BAIRD:
Q. Okay. Last question or set of questions:
Had you ever heard of a company called Centripetal
Networks before this lawsuit?
A. I had not.
Q. In developing StealthWatch, have you ever referred to or relied on anything in any way, shape, or form from Centripetal?
A. I have not. Trial Tr. 2196:2-9.

Therefore he would not have been involved in the exchange of technology between Cisco and Centripetal which resulted in integrating the new version of StealthWatch with CTA. He confirmed this on his cross examination by Centripetal:

BY MR. ANDRE (Centripetal counsel):
Q. You don't know what goes on over in Cognitive Threat

Analytics, do you?
A. I do not, just the big picture. Trial Tr. 2205:20-22.

Cisco continued to improve its security software after the June 20, 2017 transformation from manual after the fact security software to Centripetal's patented proactive machine learning security software. Llewallyn's testimony and PTX-569 illustrate the transition:

BY MR. ANDRE:
Q. I'm not asking about automatic. I'm just saying can the switches and routers -- and particularly the Catalyst 9000 switches and the same routers -- can they block bad traffic from coming in based on StealthWatch intelligence that it gives to them via the ISE?
A. That's correct. If the manual quarantine is fired, then the result is those switches or routers do initiate the rerouting of this IP address's traffic into a quarantined area, yeah.
Q. And so the switches and routers would not let this bad website get to the host, right, if StealthWatch gives it the information?
A. Well, yes. It's more like the host is quarantined, so it won't be able to reach that host anymore. The host is kind of segmented off into an area that can do no harm.
Q. And in that way, StealthWatch is being proactive in prohibiting the attack, correct?
A. I don't know about the word "proactive." It's just -- it's the result of the manual operation of the ISE quarantine. You can call that proactive, I guess, but it's in response, though, to me. You're implying to me that it's -- "proactive" to me means before, you know. This is after the fact. Trial Tr. 2202:5-2203:2.

and:

BY MR. ANDRE:
Q. Now, you talked about how StealthWatch works to monitor internal in the network, correct?
A. That's correct.
Q. You also mentioned how it is integrated with Cisco's Identity Services Engine, right?
A. That's correct.
Q. Okay. Let's go to Page Bates number 803 of this document. And in the left-hand column, there's a paragraph next-from-the-last on the bottom. It says, "Integration of Cisco StealthWatch with Cisco's Identity Services Engine." Do you see that?
A. Yes, sir.
Q. It says, "Helps organizations get 360-degree view of their extended network." Now, what I want to focus on is at the bottom, where it says, "Simplify segmentation throughout your network with centralized control and policy enforcement and address threats faster, both proactively with threat detection and

retroactively via advanced forensics." Now, StealthWatch, working with other products in Cisco's Security Suite, in this case the Identity Services Engine, can proactively protect against threats, correct?
A. Well, it's based on a manual operation, though. Trial Tr. 2198:15-2199:13.

Llewallyn describes a manual operation and he also states that there is no correlation between StealthWatch alarms and CTA alarms. However, Cisco examined Mr. Llewallyn regarding PTX-569, a 2018 Cisco technical document, as follows:

BY MR. BAIRD (Cisco counsel):
Q. And so, Mr. Llewallyn, is it true that this is a 2018 document?
A. Yes, it is.
Q. Okay. And what is this document? Is the document still used today for -- by Cisco?
A. Yes, it is. It's on the Cisco website in the public area.
Q. Okay. And what is this document?
A. It's basically how to configure your switches or routers and exporting devices to work more effectively with StealthWatch. And it also has some troubleshooting issues that you can refer to when working with StealthWatch if you see problems. Trial Tr. 2178:8-21.

Exhibit PTX-569 contains the following language:

"Cisco StealthWatch Enterprise

Cisco StealthWatch is a security analytics solution that leverages enterprise telemetry from the existing network or public cloud infrastructure. It provides advanced threat detection, accelerated threat responses and simplified network segmentation using multi-layer machine learning and entity modeling. With a single, agentless solution, you get visibility across the extended network including endpoints, branch, data center and cloud. And it is the only product that can detect malware in encrypted traffic and ensure policy compliance, without decryption.

It consumes information about the traffic that is passing through the devices in the network such as routers, switches, and firewalls. StealthWatch can analyze enterprise telemetry from any source (NetFlow, IPFIC, sFlow, other Layer 7 protocols) across the extended network, to provide real time visibility into assets that are using the network, while profiling each of these assets. It provides visibility into the east-west traffic in an enterprise network (in addition to north-south traffic) and analyzes network behavior to detect policy violations, anomalies as well as data consumption in the network. This document covers StealthWatch configuration for NetFlow enabled network devices.

Aggregation and correlation

> The flow or telemetry represents unidirectional accounting information about the traffic that is passing through a network device and is stored at the level of the flow capable device for a period of time until timeout or until flow ends. This flow will them be exported into StealthWatch that will correlate flows from multiple devices and interfaces and perform stitching and de-duplication action to provide a single bidirectional flow of the traffic end-to-end." PTX-569 at Bates No. 270.

Cisco's counsel did not identify the foregoing language from PTX-569, but they did question Llewallyn about certain other language.

> "The Flow Collector usually only needs ingress export from all interfaces on the exporter to create interface traffic data for inbound and outbound traffic. For devices that use logical interfaces enabling both may cause the Flow Collector to double report traffic stats in noninterface documents. We usually ask the Customer to choose which data set is most important." PTX-569 at Bates No. 282.

However, Llewallyn also testified:

> BY MR. BAIRD:
> Q. Okay. Have you done anything in the code to deal with that problem?
> A. I have. Some customers do export ingress/egress for their own reasons, and I've added the ability to configure the StealthWatch Flow Collector to ignore the egress side. Trial Tr. 2173:4-8.

The above testimony confirms that the egress portion of the infringing technology is also used by his customers.

Paragraph 9 of the Llewallyn affidavit is troublesome. It describes proxy as a device and a different type of equipment, when in reality proxy is more correctly classified as a software feature achieved by combining StealthWatch and CTA. The proxy sources are identified as Cisco USA, Bluecoat proxy, Squid and McAfee Web Gateway which are sources of intelligence transmitted over the internet by subscription. The Cisco product described in PTX-569 does not require any additional device or equipment to consume this data as the capability is contained in the Centripetal software embedded in Cisco's hardware as shown in the Cisco diagram in PTX-1065 attached to

Llewallyn's affidavit. *See* PTX-1065, Attachment 1 to exhibit A of Cisco's Motion for a New Trial, Doc. 625. This Cisco diagram is also cited by the Court on p.76 of the October 5, 2020 Opinion.

Paragraph 11 of the Llewallyn affidavit says the third party intelligence data does not originate in the switches and routers, which is true, but misleading. Instead this outside the network third party data enters as proxy data which is then forwarded via the switches and routers which utilize Centripetal software to correlate the proxy data with the NetFlow data thereby creating the data to be analyzed by cognitive (threat) analysis as shown in the diagram on page 5 of the Llewallyn affidavit. Llewallyn described the diagramed process in his trial testimony:

> BY MR. BAIRD:
> Q. Okay. Mr. Llewallyn, can you just briefly orient the Court about how this relates to the demonstrative that we were using earlier? Let's just start on the left side. What's this client server and this switch-router?
> A. The client server equates to computer A and computer B and the other screens. So the client is sending a request to the server above, and it's going through a switch or router to do that. As it passes through the switch or router, the NetFlow is exported to the Flow Collector to make StealthWatch flow out of it, like we were saying, and that copy of the StealthWatch flow is sent to CTA in the cloud for analysis, and then the same copy is sent to the database below for the Flow Collector, and CTA analyzes it, and it reports back to the StealthWatch Management Console anything that it discovered in terms of maliciousness.
> The StealthWatch user on the right, Adam the Analyst, he's using the user interface provided by the StealthWatch Management Console. Trial Tr. 2189:10-2090:4.

By 2018 Cisco had replaced Adam the Analyst with Centripetal's machine learning as previously explained by PTX-569.

The balance of the Llewallyn affidavit repeats Cisco's contentions that it didn't make, use, offer to sell or sell infringing products from 2017 through June of 2020. In their invalidity evidence

Cisco nonetheless claimed they possessed and offered for sale the infringing technology in 2014 and earlier which conflicts with Mr. Llewallyn's and Mr. Jones' trial testimony as well as with multiple Cisco technical and marketing documents. In its Rule 52(b)/54(b) motion alleges that Centripetal did not prove that Cisco directly infringed the '856 Patent. For the reasons stated in this Section V and in Section IV supra the Court **FINDS** that Cisco did so infringe and **DENIES** this portion of Cisco's motions based upon its claimed noninfringement of the '856 Patent.

VI. MR. JONES AFFIDAVIT AND PATENT '806

The conflict between Cisco distinguished engineer Mr. Peter Jones' trial testimony and Cisco's presentation of its expert trial testimony was a subject of the "Overview of the Evidence" beginning on page 22 of the October 5, 2020 Opinion. Cisco now seeks to supplement or perhaps to change or obfuscate his trial testimony through one of its sua sponte arguments in both its Rule 52(b)/54(b) and 59(a) motions. Initially, the Court observes there is no persuasive authority presented in support of supplementing his testimony posttrial via affidavits. However, an examination of the Jones affidavit's content discloses that it did not change his description of the functionality of Cisco's accused products, which infringe the claims in the '806 Patent referred to at trial as the "Rule Swap Patent." As the Court noted in its opinion, at trial Cisco attempted to contradict its own distinguished engineer Jones' testimony through its retained expert, Dr. Reddy. However, the Court rejected Reddy's testimony and accepted Jones' explanation, which was in accord with the other evidence introduced by Centripetal and its experts.

Jones defines the Access Control List (ACL) as a set of rules:

BY MR. POWERS (Cisco counsel):
Q. Okay. Could you briefly explain to the Court what an Access Control List is?

A. An Access Control List is basically a set of rules. Each rule contains criteria to compare a packet against and an [sic] action. Something to do. Simple actions are either to permit or deny, allow a packet to proceed forward or to throw it away. Trial Tr. 2549:24-2550:4.

The UADP is the Cisco diagram illustrated on page 28 of the October 5, 2020 Opinion (DTX-562 at Bates No. 043). Mr. Jones thoroughly explained this Cisco software which the Court found infringed the '806 Patent in DTX-562 as follows:

By MR. POWERS (Cisco counsel):
Q. Okay. Now, just to the left, there's something called the egress forwarding controller. Please tell the Court what the forwarding controller is.
A. It looks at the headers of the packets, applies the rules to them. It decides the fate of the packets.
Q. And just above that, there's something called the PBC, packet buffers complex. Do you see that?
A. I do.
Q. And could you give the Court an overview of what that component is and how it's used during packet processing?
A. That is where the packets stay, waiting for the results from the ingress forwarding controller.
Q. Do all packets pass through that buffer complex?
A. They do.
Q. Please explain any relationship between the packet buffers complex and the hitless ACL rule update technique that we talked about yesterday.
A. There is no relationship.
Q. Now, if we go to the bottom left-hand corner, there is something called ingress FIFO.
THE COURT: What is that packet buffers complex? What is that?
THE WITNESS: It is a storage place. So as packets arrive in from ports, the packet headers are sent to the ingress forwarding controller. The packet itself goes into the packet buffers complex.
THE COURT: What goes there?
THE WITNESS: I'm sorry. Could you repeat yourself, Your Honor?
THE COURT: What goes from the ingress forwarding controller to the packet buffers complex? What goes there?
THE WITNESS: The results of all the rule settings, so the instructions for what to do with the packet. A simple case would be throw the packet away. Another one would be send it to the stack interface or the ingress forwarding controller.
THE COURT: The second one would be what, now?

THE WITNESS: A very simple answer would be if the rule set at the ACL says to discard the packet, the instruction would go from the ingress forwarding controller to the packet buffer to discard the packet.
THE COURT: And you said the second alternative was what?
THE WITNESS: It would be to send the packet forward, to send it out to a different forwarder or switch so it could leave.
THE COURT: So it could what?
THE WITNESS: A way to describe this would be the results of like a -- of an ACL could be either to admit or deny. The ingress forwarding controller processes those rules. It may send an instruction to the packet buffers complex to discard the packet, or it may send an instruction to tell the packet buffers complex where that packet should leave the system.
THE COURT: So if it goes to the packet buffers complex, it's not going to reach its destination --
THE WITNESS: Let me clarify.
THE COURT: -- its original destination; is that right?
THE WITNESS: Let me clarity. The packet buffers complex is where the packet stays waiting for results from the ingress forwarding controller. It may be dropped, or it may be sent on to its destination. For instance, you will see on the right-hand side there's links from the packet buffers complex to the egress forwarding controller. This is the part in which the packet can leave the system.
THE COURT: Well, when you say, "leave the system," that means it's been blocked; is that right?
THE WITNESS: No, that does not mean it's been blocked. If it has been blocked, it is discarded. If we forward the packet, it will leave out another port on the system. It's an example of the path on which it would leave.
THE COURT: But there might be different paths that it would follow. Is that right?
THE WITNESS: So we have a number of these complexes inside the system. This would describe when the ingress port and the egress port were on the same UADP. The block at the top -- you see it's called "stack interface" -- this is how we link together multiple UADPs inside the system. So the results of the ingress forwarding controller can include a set of destinations that the packet needs to leave the system.
THE COURT: Well, suppose it was going to go to its destination, initial destination. Where would it go from the packet buffers complex? Would it go through the ingress forwarding controller?
THE WITNESS: No. If you see, it would not – it would leave through the egress forwarding controller. We tend to have -- the ingress forwarding controller is the processing we do on packets as they arrive. The egress forwarding controller is the process we do on the packets as they leave the system.
THE COURT: Well, maybe I'm not understanding what it means to leave the system. When you say, "leave the system," where does it go when it leaves the system?
THE WITNESS: It will go out one of the ports. On the front of the switch, you'll see a whole set of ports. So packets arrive through a port and are processed. While they're waiting for the result, they sit in the packet buffers complex. Once we have

the results, which could either be throw the packet away or forward the packet, it will leave out through one of our egress forwarding controllers out to a port.
THE COURT: And will it go from the egress forwarding controller to the original destination?
THE WITNESS: Yes. Trial Tr. 2563:2-2567:8.

Jones repeated this same explanation a second time in his direct testimony:

By MR. POWERS(Cisco counsel):
Q. And, Mr. Jones, could you just remind us what FIFO is?
A. It's called a first-in-first-out buffer. It's a small queue.
The packet is then sent into the PBC for storage.
Q. What is the PBC?
A. Yes.
Q. Could you -- packet buffers complex?
A. Packet buffers complex.
Q. Thank you.
A. At the same time, the packet headers, the addresses of the packets, are sent into the ingress forwarding controller. The ingress forwarding controller processes the packet according to the rules that are in the lookup tables. The result is then sent to the packet buffers complex, and it instructs the packet buffers complex what to do with the packet. A simple example would be to throw the packet away. Another example would be to send it out a port. If the packet is to be sent out a port, it's sent from the packet buffers complex to the egress forwarding controller. The egress forwarding controller also runs rules, including Access Control Lists. When the packet is finished going through the egress forwarding controller, it could also be dropped, or it could be sent out a port. It goes via the rewrite engine, which makes modifications to the packets. It goes through the egress FIFO, again, a small shallow buffer, the block level MACSec, Media Access Control Security -- it's an encryption block -- and the packet would leave the front panel port. So it comes in on the left side, circles around, and goes out on the right side. Trial Tr. 2568:1-2569:9.

And again repeated the same explanation during his very brief cross examination by Centripetal:

BY MR. HANNAH (Centripetal counsel):
Q. Thank you, Your Honor. Good morning, Mr. Jones.
A. Good morning.
Q. My name is James Hannah. I'll be asking you some questions this morning. I want to talk about the Catalyst switches that
you've been discussing and, in particular, the 9000 series of
switches, okay?
A. Yes.
Q. Now, the Catalyst switches, they can receive rule sets from a variety of sources; isn't that right?

A. That is correct.
Q. And one of those sources can be the DNA center; isn't that right?
A. Yes, they may receive rules from the DNA center.
Q. And, now, the way the Catalyst processes these rules, in order to process these rules, the Catalyst switch must compile them, right, in order to implement the rules?
A. That is correct.
Q. And in doing this compiling, it compiles these rules while the old rule set is still processing packets, while the old rules are still being applied to packets; isn't that right?
A. That is correct.
Q. Now, once the compilation is complete, a signal is sent to the processor to stop processing packets with the old rule set and to start processing packets with the new rule set; isn't that right?
A. That is correct.
Q. And then during the two to four clock periods that you mentioned yesterday, when there's no processing of packets, the rules are swapped; isn't that right?
A. That is correct. There is -- the processing of packets continues. Packets are processed at a maximum frequency of two to four clock periods. So we don't stop processing the packets, there's just an idle period between two packets.
Q. But there's a signal that's sent to say, stop processing packets with the old rule set and start processing packets with the new rule set, correct?
A. Yes, we swap from the old to the new.
Q. And you do that swap in between -- in that two to four clock cycles that you mentioned yesterday, correct?
A. Right.
Q. Now, once that process is complete, the system signals that the swap has been complete, and then the new rule set will be applied to any subsequent packet; isn't that right?
A. We don't -- we don't signal that a swap is complete, we just instruct the swap to happen.
Q. Well, there's a return success that happens after the swap is complete, correct?
A. There's really not. We just do a write of the new value.
So it's a memory write.
Q. A memory write, okay. But in the document, it actually says that you return success. That's how you represent that memory write, correct?
A. Yes.
MR. HANNAH: No further questions, Your Honor. Trial Tr. 2571:2-2573:9

Mr. Jones affidavit in paragraphs 8-12 outlines what "he could have testified to." While no persuasive authority is cited for such content to be considered, there is nothing in paragraphs 8-12 to contradict what "he did testify to" at trial. As it did during trial with its expert witness, Dr. Reddy, Cisco is attempting to contradict or obfuscate Jones' trial testimony upon which the Court

relied. Cisco's principal defense to infringement of the '806 Patent during the trial was that it's accused products neither cached (stored) the packets nor subjected them to two sets of rules during processing. Jones' trial testimony, which is not contradicted in his affidavit, confirms that Cisco's accused products "store packets in the buffer" (the same function is referred to in the trial as "caches") between subjecting each packet to a first set of rules on ingress and a second on egress.

As is explained in more detail in its October 5, 2020 Opinion, Jones' testimony corroborated Centripetal's own expert testimony and the Court accordingly DENIES both Cisco's Rule 52b/54b and its 59(a)(2) motion insofar as they are based upon its alleged noninfringement of the '806 Patent.

VII. CISCO'S ADDITIONAL EVIDENCE

Centripetal has cited multiple circuits and other federal courts that have refused to accept additional evidence of the nature proffered by Cisco before this Court in post-trial motions, and Cisco has not cited any applicable authority to the contrary. Nonetheless, the Court has reviewed and considered the affidavits of Mr. Llewallyn and Mr. Jones and finds that there is no content therein or content in the attachments to Mr. Llewallyn's affidavit that would change the Court's interpretation of their trial testimony and the inferences to be drawn therefrom. Cisco has also cited testimony from the trial in its briefs, much of which the Court rejected and instead adopted testimony presented by Centripetal to the contrary. In addition, in numerous portions of their opening and Reply (Rebuttal) briefs, Cisco presents testimonial statements, without reference to trial testimony or exhibits that the Court admitted. Such testimonial statements are given no weight by the Court, as there are no evidentiary references to support the same.

As Centripetal argued, with supporting authorities, in its brief: Cisco cannot simply add evidence that was not introduced at trial. *See Goldblum v. Klem*, 510 F.3d 204, 226 n.14 (3d Cir. 2007) ("Evidence is not 'new' if it was available at trial, but a petitioner merely chose not to present it to the jury."); *see also*, *Amrine v. Bowersox*, 238 F.3d 1023, 1029 (8th Cir. 2001), cert. denied, 534 U.S. 963 (2001) (approving district court's determination on remand that "evidence is new only if it was not available at trial and could not have been discovered earlier through the exercise of due diligence"); *United States v. Starr*, 275 F. App'x 788, 790 (10th Cir. 2008) ("[T]he district court correctly found that this evidence was available before trial, and in fact had been discovered by defense counsel. Thus Starr's claim is not based on 'new' evidence, but rather on evidence that could have been presented at trial.").

Numerous federal trial courts cited by Centripetal have come to the same conclusion. *See, e.g.*, *Berlinger v. Wells Fargo*, N.A., No. 2:11-cv-459-FtM-29CM, 2016 WL 11423815, at *1 (M.D. Fla. Sept. 6, 2016); *Guisao v. Secretary, Dep't of Corr.*, No. 8:15-cv-9-T35AAS, 2018 WL 10883771, at *2 (M.D. Fla. Mar. 26, 2018); *Lorme v. Delta Air Lines, Inc.*, No. 03-cv-5239 (GBD), 2005 WL 1653871, at *5 n.6 (S.D.N.Y. July 13, 2005); *Watkins v. Casiano*, No. CCB-07-2419, 2009 WL 2578984, at *3 (D. Md. Aug. 17, 2009), aff'd, 413 F. App'x 568 (4th Cir. 2011); *Connelly v. Blot*, No. 1:16-cv-1282 (AJT/JFA), 2017 WL 11501501, at *3 (E.D. Va. Oct. 18, 2017). Cisco has not provided any authority to the contrary. The one case cited by Cisco, *Twigg v. Norton Co.*, 894 F.2d 672, 675-676 (4th Cir. 1990), does not support the admissibility of the Llewallyn affidavit or its attachments, the Jones affidavit, or the testimonial statements in Cisco memoranda, and accordingly this Court **FINDS** that such evidence is not admissible for purposes of the Cisco motions ruled upon in this opinion and order. In its October 5, 2020 Opinion the Court

found direct infringement of the four (4) patents based upon Centripetal's evidence. It further found that the functionality explained in Cisco's own evidence as to the '806 Patent based upon Mr. Jones' testimony and Cisco's documents would also support infringement under Centripetal's evidence. It was not a sua sponte finding as Cisco's purported defense amounted to an admission of infringement set forth by its own distinguished engineer, Mr. Jones and corroborated by Cisco's technical publications.

In its other motion under Rules 52(b) and 54(b), Cisco claims that Centripetal did not prove Cisco's hardware was embedded with Centripetal's technology or sold in combination with same. Interestingly, Cisco states in its Reply (Rebuttal) brief in support of its Rule 52(b)/54(b) motion "... but Cisco only admitted that it loaded software onto "some" of the accused firewalls in the United States," which is, of course, all Centripetal has to prove in the making, using, and selling factor of its infringement case against the firewalls. The factor of sales of the accused products embedded and used in combination as for damages is analyzed in Section IV of this opinion. Accordingly, the Court **DENIES** Cisco's motion insofar as it is based upon the noninfringement of the '806 Patent as argued in both Rule 59(a)(2) and 53(b)/54(b) motions.

VIII. THE '193 PATENT

Cisco challenges the Court's finding that the accused products directly infringed the '193 Patent in its Rule 52(b)/54(b) motion. It alleges in its motion that the Court's finding of direct infringement depends upon the theory that the Identity Services Engine (ISE) device must be found to infringe. The use of the word engine may suggest that ISE is a "device," but in reality it is a

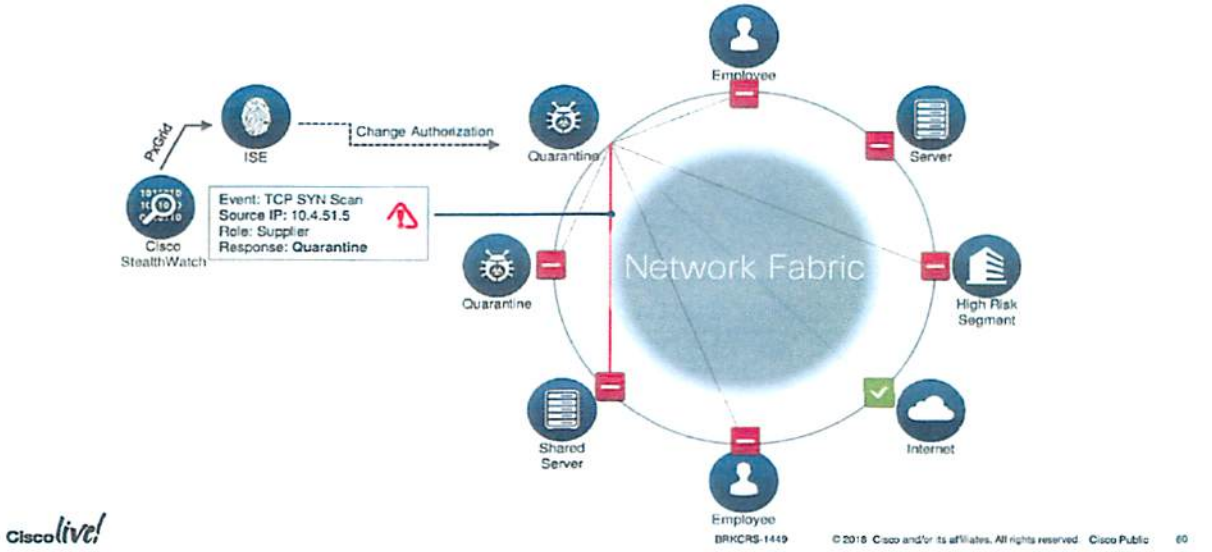
part of Cisco's infringing software. The Court did describe ISE as a "device" in patent jargon on Page 19 of the October 5, 2020 Opinion.

Cisco states "However, Centripetal's infringement proof also relied extensively on ISE to establish infringement of the '193 Patent." Doc 628 at 9. Actually, Centripetal's expert Dr. Mitzenmacher's testimony was to the contrary.

> BY MR. GAUDET (Cisco counsel):
> Q. Dr. Mitzenmacher, you didn't undertake any analysis to figure out how many of Cisco's router and switch customers also buy StealthWatch or also buy Cognitive Threat Analytics or also buy the Identity Services Engine. You don't know any of those numbers. Is that fair?
> A. I certainly couldn't recite them to you. Off the top of my head, I don't know them, but, again, since these are both system claims and computer-readable medium claims, which relate to the code on the switches and the performance of the switches and all our end routers, and all of these devices have the code there to do these things, as I've described, I just am not clear why that would specifically be relevant for me, but... Trial Tr. 804:11-23.

Cisco also states: "Again, the Court did not find that Cisco's switches and routers are only ever used with ISE, and the record would not support such a finding." Doc. 628 at 9.

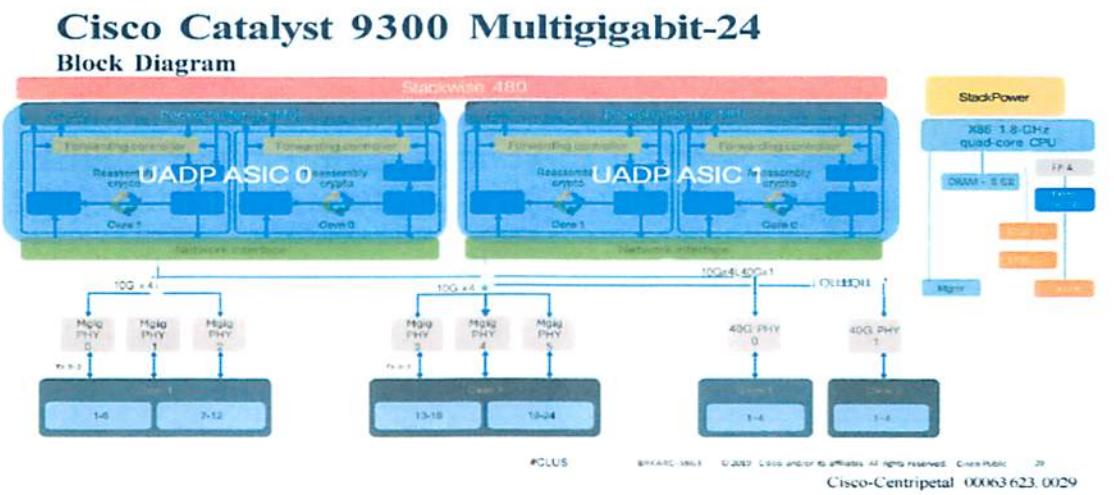
While it is not clear to the Court precisely what this sentence means, Ex. PTX-563, a Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenmacher (Tr. at 500) at Page Bates No. 415, diagrams StealthWatch forwarding data to ISE which in turn forwards data to the switches and routers in which the infringing software is embedded as explained by Dr. Mitzenmacher.

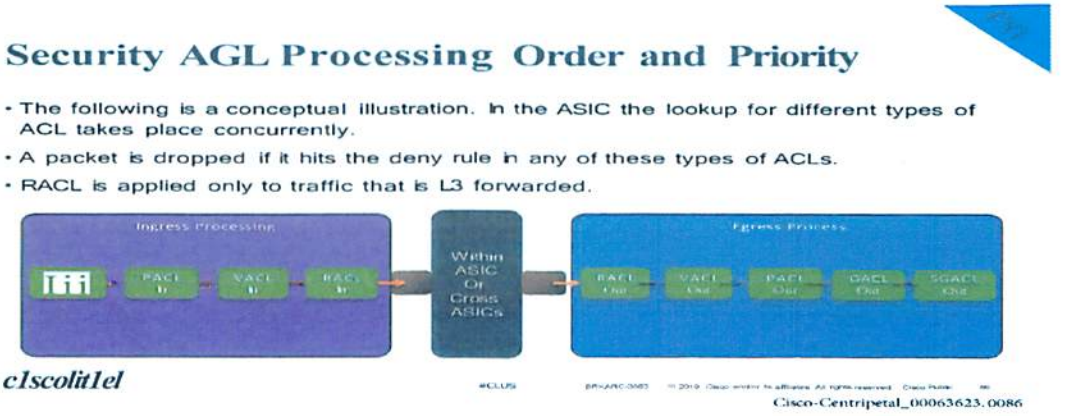


The language from PTX-1280, also a 2018 Cisco technical document introduced by Centripetal during the testimony of Dr. Mitzenmacher, contains the following language confirming that the switches and routers perform a two stage process as opposed to only one stage which was Cisco's defense to infringement at trial:

> "Notice above that rapid threat containment is seamless in SD-Access fabric, as the endpoint continues to be operational in the employee VLAN and the IP address remains unchanged. However, the SGT assignment has changed from 4 to 255, which is the quarantine SGT.
>
> Fabric edge devices will then download SGACL permissions specific to SGT 255, which will limit the endpoint's network address access until a successful remediation is performed." PTX-1280 at Bates No. 21.

Exhibit PTX-1390, a 2019 Cisco technical document, introduced by Centripetal, illustrates at Bates No. 029 how the packets are buffered between being subjected to the two-step process and at Bates No. 086 how the packets are subjected to one set of ACLs (rules) at stage one and, after being placed in the buffer, another set of ACLs on egress at stage two. As to the '193 Patent, this exhibit corroborates the infringing software embedded in Cisco's switches and routers processes the data sent to them by ISE and StealthWatch via a two stage process.





As it did at trial, Cisco attempts to ignore the content of its technical documents that Centripetal introduced in evidence as well as the clear inferences to be drawn from them. In its Reply (Rebuttal) brief in support of its 59(a)(2) motion, Cisco argues that "… Cisco also would have offered factual testimony from the many Cisco technical witnesses that were the original architects of the relevant products." Doc. 635 at 15, line 20. The Court repeatedly observed in the October 5, 2020 Opinion that Cisco failed to call such technical witnesses to respond to its technical documents which Centripetal presented as exhibits. The Court inferred in its October 5,

2020 Opinion on page 159 that Cisco wished to protect such witnesses from Centripetal's cross examination. Cisco goes on to argue in its Reply (Rebuttal) brief in Doc. 635 page 15 line 22, "For example, Cisco would have elicited testimony confirming that – contrary to the Court's findings (Order at 140-141) the increase in sales was impacted by the addition of numerous non-accused features, and had nothing to do with Centripetal's claimed technology." Cisco's marketing documents raved about its increased sales based upon the functionality of the accused products. If Cisco actually had evidence of such new and non-accused features in its hardware or in its own software, why would it not present it at trial?

FRCP 52(b) motions should not attempt to relitigate a theory available at trial. The rule states that a party may make a motion requesting the Court "amend its findings—or make additional findings—and . . . amend the judgment accordingly." "The purpose of motions to amend is to correct manifest errors of law or fact or, in some limited situations, to present newly discovered evidence." *Fontenot v. Mesa Petroleum Co.*, 791 F. 2d 1207, 1219 (5th Cir. 1986) (quoting *Evans, Inc. v. Tiffany & Co.*, 416 F. Supp. 224, 244 (N.D.Ill.1976)). "This is not to say, however, that a motion to amend should be employed to introduce evidence that was available at trial but was not proffered, to relitigate old issues, to advance new theories, or to secure a rehearing on the merits." *Id.* (citing *Evans, Inc. v. Tiffany & Co.*, 416 F. Supp. 224, 244 (N.D.Ill.1976)). Additionally, as Centripetal argues in its opposition brief, a Rule 52(b) motion should not be granted when it "constitute[s] nothing more than an invitation to the district court to reverse itself." *Weatherchem Corp. v. J.L. Clark, Inc.*, 163 F.3d 1326, 1336 (Fed. Cir. 1998) (denying motion). Doc. 630 at 4. Accordingly insofar as its Rule 52(b)/54(b) motion relies on Centripetal's alleged failure to prove direct infringement of the '193 Patent, such motion is **DENIED**.

IX. THE '176 PATENT

Cisco challenged the Court's ruling that the '176 Patent was infringed by the accused products in both its Rule 52(b)/Rule 54(b) motion and its Rule 59(a)(2) motion. The '176 Patent was referred to during the trial as the "Correlation Patent."

In its Rule 52(b) / 54(b) Reply (Rebuttal) brief there is only a single paragraph referencing the '176 Patent. The argument is based upon Cisco's made, used, or sold in combination argument which the Court analyzed in Section IV of this opinion. Again, Cisco begins its argument in its Rule 59(a)(2) opening brief by stating "The Court sua sponte adopted a new claim construction and infringement theory with regard to the '176 Patent." Doc. 626 at 2. Cisco argues that Dr. Cole limited his infringing testimony to a single switch or router. Dr. Cole's cross examination testimony does not support Cisco's claim; indeed it may suggest exactly the opposite:

> BY MR. JAMESON (Cisco counsel):
> Q: Now Dr. Cole, this is claim 11 [of the '176 Patent], all right?
> A: Once again we have the same caveat that this is the exact wording from the patent and nothing's been altered or modified.
> Q: Okay. And if you look at the elements B1 through B4, there is a reference to a network device in each of those elements, right?
> A: That is correct. There is a network device listed in each of those elements.
> Q: And the network device is the router or switch, right?
> A: Once again, we're not infringing individual components, it's the entire system, but the *component* in this case that's receiving and transmitting those packets is the router or switch. Trial Tr. 1101:1-13 (emphasis added).

In any event Centripetal dealt directly with this point when Cisco's expert witness on the '176 Patent, Dr. Almeroth testified during his cross examination as follows:

> BY MR. KASTENS (Centripetal counsel):
> Q. And then you said this had to be a single network device, correct?

> A. Not quite. It says a network device here, and then later it's the network device. So it's the same network device across the limitations.
> Q. But you do understand that in a patent, when it says A, it can mean one or more; is that correct?
> A. That's my understanding.
> Q. So this could be more than one network device, correct?
> A. It could be. Trial Tr. 2278:11-20.

Mr. Llewallyn also corroborated Centripetal's claim that multiple switches and routers are utilized in Cisco's infringing network:

> BY MR. BAIRD:
> Q. Now, this slide just showed one router or switch. Mr. Llewallyn, is it correct that the flow collector could be getting NetFlow records from other switches and routers along the path between the two computers that aren't shown here?
> A. That's correct. And it's also most common. It's very rare to get it from just one. Trial Tr. 2149:12-18.

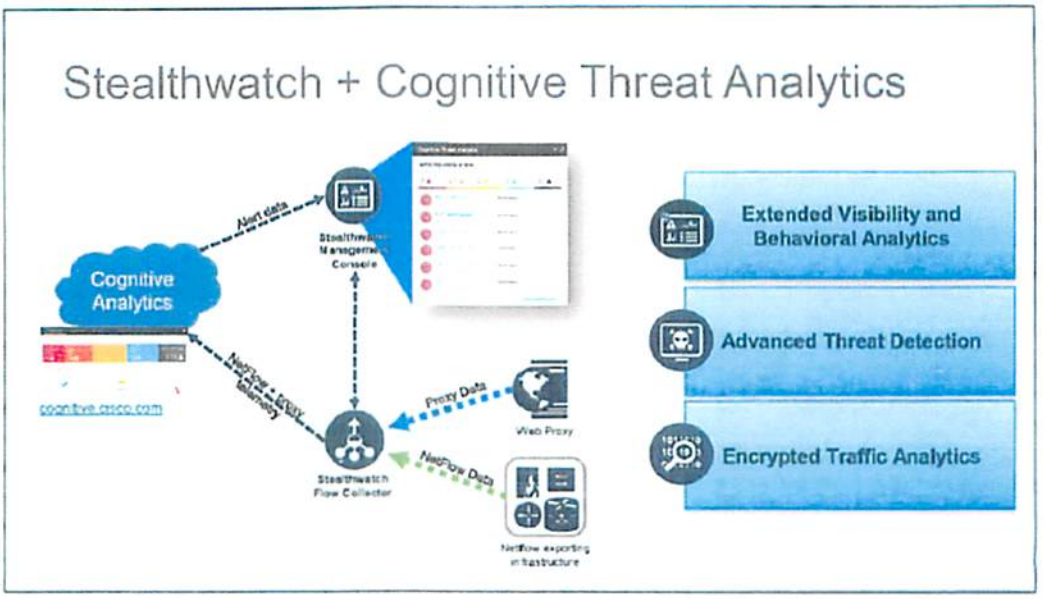
The multiple device language also appears in the patent specification. *See* '176 Patent col.2 l.58-63 (filed Jan. 31, 2017) ("Network device(s) **120** may include one or more devices (e.g., servers, routers, gateways, switches, access points, or the like) that interface hosts **108**, **110**, and **112** with network **106**. Similarly, network device(s) **122** may include one or more devices that interface hosts **114**, **116**, and **118** with network **106**."). Therefore, it was Centripetal and its exhibits that introduced the multiple device argument, not the Court sua sponte. Notably "devices" as used in the patent means; servers, routers, gateways, switches, access points (another name for firewalls) or the like, all expressed in the plural.

Cisco's repeated references to sua sponte seems to suggest that the Court must somehow limit its analysis to the testimony of Centripetal's experts. The Court again observes that Cisco's own documents contradict its arguments, in particular PTX-1065 a November 2017 Cisco

technical document which is Exhibit A to Mr. Llewallyn's affidavit Doc. 635, Ex. A, Attachment 1.

Compare Cisco's argument in its "Reply" (Rebuttal) brief:

> "Had Centripetal or its infringement expert relied on a "one or more" construction of the phrase "a network device," then Dr. Almeroth would have explained why that theory breaks down as well—namely that the claims would still require correlation of packets received into a set of switches or routers with packets transmitted by the *same* set of devices; not just any "correlation" generically with other data. Finding a document with the word "correlation" in it is not good enough; the claims requires correlation of packets entering with packets exiting the same thing. Had Centripetal accused a group of switches or routers, Dr. Almeroth could have responded accordingly. But because Centripetal did not raise the Court's new theory, Cisco had no notice of it and no opportunity to present responsive evidence at trial.
>
> Finally, Centripetal's suggestion that its expert Dr. Cole testified regarding correlation of logs from multiple devices is incorrect. *See* Opp. at 10. Centripetal cites a brief discussion of Syslog data in Dr. Cole's redirect examination, which contains no suggestion that StealthWatch can correlate logs from multiple switches or routers. Trial Tr. 1114:24-1116:20. More importantly, the cited testimony actually shows that Dr. Cole *does not* use Syslog as evidence of infringement. Dr. Cole testified: So customers can just use NetFlow by itself to do that correlation. It does not need to use the proxy data." *Id.* at 1116:12-13. When asked what this means for infringement, Dr. Cole testified "This shows that the claim language says *it must be able to correlate the two NetFlows*. So this is confirming that it can correlate NetFlow by itself which would consist of ingress and egress NetFlow." *Id.* at 1116:23-1117:1 (emphasis added). In sum, Dr. Cole never opined that correlation of Syslogs is infringing; his infringement theory relied entirely on correlation of NetFlow data." Doc. 635 at 6.



Stealthwatch integrates with Cognitive Analytics ("CA" - aka Cognitive Threat Analytics). This involves the addition of a new information panel on the SMC's WebUI, and enhances Stealthwatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time.

Compare the foregoing argument by Cisco with its 2017 technical document PTX-1065. The explanatory text contains the following language which explains the functionality of the diagrammed Cisco network which infringes as made, used, and sold by Cisco and contradicts its arguments:

> "…and enhances StealthWatch further by leveraging CA's cloud based analytics engine, that correlates threat behaviors seen in the enterprise with those seen globally. It uses machine learning and statistical modeling to learn from what it sees and adapt to changing network behavior over time…
>
> …This solution uses the Proxy ingestion feature to consume Syslog information sent from proxy sources, integrating it into StealthWatch's flow visibility…
>
> …This Syslog information contains details similar to what a flow record contains: Source IP, destination IP, Source Port, Destination Port, URL, Username…

> ...StealthWatch will then correlate the received Syslog and relates it to the flows collected from network devices before and after the proxy, providing deeper visibility into customers web traffic...
>
> ...Customer may use either NetFlow or Proxy data, or both..." PTX-1065 at Bates No. 005.

In support of its arguments Cisco attacks a part of PTX-1065 in the text of Mr. Llewallyn's affidavit at Paragraph 11 on Page 5, Doc. 626-1. The explanatory language which appears immediately below the diagram in PTX-1065 as it was introduced at trial contains the foregoing explanatory language that directly contradicts both Mr. Llewallyn's affidavit and Cisco's argument in its Reply (Rebuttal) brief as well as the testimony of Dr. Almeroth, Cisco's expert witness on the '176 Patent. (Exhibit 1065 in its entirety is attached to Cisco's brief Doc. 626-1 as Exhibit A).

Attachments 2 and 3 of Mr. Llewallyn's affidavit amount to no more than a play on words. These exhibits use the term "de-duplicated," which is a function performed by a previous form of StealthWatch when Lancope was still a separate company, as if it described the accused technology, which it does not. De-duplication is only one of the many functions of the post June 20, 2017 infringing software. The term de-duplication does not even appear in the diagram or the text explaining the diagram. Likewise, the Llewallyn affidavit states that "proxy data" in PTX-1065 is not "generated" by Cisco's switches and routers, which is correct, but, again, misleading. The proxy data, which is intelligence data usually generated by third parties, arrives at Cisco's network via the internet whereupon Cisco switches and routers (single as shown in the diagram, or multiple), embedded with Centripetal's infringing technology, feed it to StealthWatch which correlates it and sends it to Cognitive Analysis (aka Cognitive Threat Analysis) and the correlated intelligence data generate rules which are utilized to process such data in its infringing network of

switches, routers and, in some instances, firewalls as well. Clearly there is more going on in Cisco's post June 20, 2017 network than "de-duplicating" as described in attachments 2 and 3.

The diagram's explanatory text demonstrate that the StealthWatch and Cognitive Threat Analysis contain either correlation from a single source through a single router (i.e. NetFlow Data to StealthWatch Flow Collector) which processes ingress, correlation and egress through a single switch (i.e. NetFlow to StealthWatch Flow Collector to Cognitive Analysis) or multiple switches, Proxy Data (such as Syslog and NetFlow Data to StealthWatch Flow Collector or Collectors to Cognitive Analysis). *See* PTX-1060.

However, PTX-1060, a Cisco technical document introduced by Centripetal during Dr, Cole's testimony, demonstrates that as of December 2017 Cisco was having scalability issues which indicate the need for multiple StealthWatch Flow Collectors describing multiple switches as follows:

> "The Catalyst 9400 series of switches supports analysis of up to 3500 flows per second for ETA and are capable of up to 384,000 NetFlow entries per switch (128K per ASIC); 192,000 ingress and 192,000 egress based on the installed supervisor regardless of the number of linecards installed. At 3500 FPS for ETA, it is recommended that it only be configured when the Catalyst 9400 is used as an access switch and not in distribution or core of the network. As with the Catalyst 9300, ETA on the 9400 when exceeding 3500 flows per second may miss exporting ETA records for some flows, causing incomplete ETA fields in flow analysis.
>
> In addition to the Catalyst 9300 and 9400 specification, you need to carefully consider the number of StealthWatch Flow Collectors required to support the Catalyst 9300s with ETA configured and the flows per second reaching the Flow Collectors." PTX-1060 p. 23.

Centripetal's demonstrative exhibit PTX-547 explains that its software technology solves Cisco's speed and reliability problems. PTX-547, page 141 of the October 5, 2020 Opinion.

Cisco argues that "Finding "a" document with the word correlation is not good enough." (emphasis added) In addition to PTX-1065, which both diagrams and explains in depth how the '176 Patent is infringed through correlation, the following Cisco technical publications post June 20, 2017 explain the correlation feature in whole or in part; PTX-584 at Bates No. 402, PTX-1009 at Bates No. 409, PTX-591 at Bates No. 522, PTX-202, PTX-569 at Bates No. 272 and PTX-1893 at Bates 011. Pre June 20, 2017 older versions of StealthWatch also used the term "correlate" (DTX-343 Bates No. 002), however, the technology at that time relied upon manual responses from Adam the Analyst and therefore operated only retroactively;

> "The StealthWatch System quickly zooms in on any unusual behavior, immediately sending an alarm to the SMC with the contextual information necessary for security personnel to take quick, decisive action to mitigate any potential damage." DTX-343 at Bates No. 001 (a 2014 document).

Cisco technical documents also illustrate that Cisco's products continued to rely on manual software referred to as "Adam the Analyst" until it copied Centripetal's machine learning software. PTX-1089 at Bates No. 239.

Cisco did not successfully copy all of Centripetal's technology at one time, rather it did so over a period of years. It now claims the ability to process billions of packets, where it formerly claimed hundreds of thousands.

Cisco cannot credibly argue that it was taken by surprise (i.e. sua sponte) by its own technical documents or by the patent itself, both of which refer to multiple devices and both of

which were introduced by Centripetal during trial. Accordingly what Cisco attempts to classify as sua sponte originated in the patent itself, was the subject of cross examination of Cisco's retained expert Dr. Almeroth as well as Cisco's direct examination of its distinguished engineer, Mr. Llewallyn, and was corroborated by Cisco's own published documents and explanatory text. The Court **DENIES** both Cisco's Rule 59(a)(2) motion and its Rule 52(b)/54(b) motion insofar as each motion relies upon its claim that Centripetal failed to prove infringement of the '176 Patent.

X. WILLFULNESS

While Cisco did not directly address willfulness in its brief in support of its Rule 59(a)(2) motion, it did argue the point in its Reply (Rebuttal) brief. The Court addressed willfulness in its October 5, 2020 Opinion in Pages 149-161 as well as on Page 166.

Cisco is particularly critical of the Court's analysis of *Read* factor four, Cisco's "size and financial condition." Cisco does not dispute the significance of its "size and financial condition, as it portrays itself as "the largest provider of network infrastructure and services for many years before any of the patents issued." Doc. 635 at Page 17.

In reviewing Cisco's marketing documents, the Court observes the repeated claims that it had "solve[d] a network security challenge previously thought to be unsolvable" (PTX-452 at Page 648) and was the "Industry's first network with the ability to find threats in encrypted traffic without decryption." (PTX-989 at Page 4); *see also*, PTX-383 ("Stealthwatch is the first and only solution in the industry that can detect malware in encrypted traffic without any decryption using Encrypted Traffic Analysis."); PTX-561; PTX-963; PTX-1004; PTX-1010; PTX-1136; PTX-1417. All the while Cisco knew that Centripetal had solved the challenge and was providing the

software needed to deal with encrypted traffic, based upon information it obtained from Centripetal during the Nondisclosure Period. The Nondisclosure Agreement was signed and effective on January 26, 2016 (PTX-99) and confidential information was shared for approximately one and a half years thereafter. Thus, Cisco utilized its footprint in the marketplace and financial prowess to the detriment of Centripetal and its conduct was willful and egregious.

XI. FINAL ORDER

The Court has undertaken to analyze each issue raised by Cisco in both of its motions individually and collectively. The Court **DENIES** the relief sought in Cisco's Rule 59(a) as it **FINDS** no merit in any of the grounds upon which Cisco relies. The Court also **FINDS** no merit in any of the grounds raised in support of its Rule 52(b)/54(b) motion when considered individually and collectively and accordingly **DENIES** that motion.

With regard to Cisco's motion as it separately relates to Rule 54(b) the Court **FINDS** that Cisco's request is mooted by the Court's Order of November 19, 2020 **GRANTING** the joint motion of the parties to dismiss, without prejudice, all remaining claims not addressed in its Order of October 5, 2020.

Therefore the Court enters **FINAL JUDGMENT** in favor of Centripetal Networks, Inc. against Cisco Systems, Inc. for the reasons and upon the terms set forth in its October 5, 2020 Order as well as in this Order.

The Clerk is **REQUESTED** to electronically deliver a copy of this Opinion and Order to all counsel of record.

It is **SO ORDERED**.

/s/
Henry Coke Morgan, Jr.
Senior United States District Judge

HENRY COKE MORGAN, JR.
SENIOR UNITED STATES DISTRICT JUDGE

March 17, 2021
Norfolk, Virginia